

REMARKS

Thorough examination of the application is sincerely appreciated.

Applicant's representative thanks the Examiner for indicating the allowability of claims 3 and 8.

The Final Office Action maintains the rejection of claims 1, 2 4-7 and 9-12 under 35 U.S.C. 103(a) as being unpatentable over Komuro et al. (USP 6,223,285, hereinafter "Komuro") and Gray et al. (USP 5,706,348, hereinafter "Gray"). The applicant respectfully traverses this rejection.

The Examiner's attention is requested to MPEP 2142, wherein it is stated:

"To establish a *prima facie* case of obviousness ... the prior art reference (or references when combined) *must teach or suggest all the claim limitations*... If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

Neither Komuro nor Gray teaches Applicant's feature of **"a key check block field that contains a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information"** as recited in independent claims 1 and 9-11 of the instant application (hereinafter referred to as "Applicant's recited feature").

It is acknowledged in the Final Office Action that "[nor] does Komuro explicitly disclose the use of a key check block that is decrypted by the candidate sink session keys until a valid result occurs." Specifically, Komuro's "EMI Extractor" 440/540, which determines which session key was used to encrypt a packet, operates directly on the received data, before any decryption is performed (Komuro's FIG. 5A/5B). It, therefore, follows that Applicant's recited feature cannot possibly be disclosed in this reference relied upon in the Final Office Action.

To cure the deficiency in Komuro, Gray is relied upon in the Final Office Action for teaching decrypting data of a received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found and causing a decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key that produced the valid decryption result. Applicant respectfully disagrees with this characterization of Gray.

As taught by Gray, a new/next decryption key is communicated to a receiver, and then transmits a marker packet that signals the commencement of the use of this new decryption key. At any point in time, Gray's system contains two decryption keys: the current key and the new key, and the choice of which to use is based on receipt of a marker packet. Of particular note, Gray's marker packet is decrypted using the current decryption key (Gray's FIG. 7, and column 6, lines 8-27 as referred to in the Final Office Action).

The identification of valid marker packets begins with the extraction (operation 100) of the values stored in the current key bit positions, the new key bit positions and the CRC bit positions in a packet's decrypted payload. A CRC value is then calculated at the destination node (operation 102) based on the data in the first "n" bit positions in the data field and compared (operation 104) to the extracted CRC value. If the calculated and extracted values are not equal, it is assumed that the packet is not a marker packet. The packet is forwarded in the destination node system for further processing in an operation 108. (emphasis added)

According to Gray, if the marker packet is not validly decrypted, it will not be recognized as the marker packet. In Gray, no additional keys will be applied to such (non-marker) packet. Gray does not teach applying a different key (the next key) to that particular packet that was previously classified as non-marker packet. Gray fails to disclose that a different key is applied until a valid decryption result is found, as recited in Applicant's claims.

For the above reason, Applicant respectfully maintains that the decryption of a marker packet using the current decryption key does not correspond to the applicant's claimed decryption of a received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found, as asserted in the Office action.

Furthermore, nowhere does Grey teach or suggest Applicant's recited feature of "a key check block field that contains a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information" as recited in independent claims 1 and 9-11 of the instant application"

In light of the above, it is respectfully submitted that a prima facie case of obviousness has not been established in the Final Office Action, and the rejection of claims 1, 2, 4-7 and 9-12 under 35 U.S.C. 103(a) over Komuro and Gray is unfounded, per MPEP 2142.

Consideration of this amendment is respectfully requested in accordance with the MPEP, section 714 .13. Applicant's claims, as amended herein, do not present new issues requiring


Serial No. 09/734,777

Page 9 of 9

further consideration or search. Applicant's recited feature was removed from claim 3, which has been examined and found allowable in previous Office Actions, and added to independent claims. Since this amendment places the application in condition for allowance, withdrawal of the final rejection is respectfully requested per MPEP 706.07(e).

However, should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned in order to facilitate reaching a resolution of any outstanding issues remain.

Respectfully submitted,

By 
Yuri Kateshov, Reg. No. 34,466
718-637-6027